JPL PUBLICATION 80-79

(NASA-CR-163911) FBI FINGERPRINT
IDENTIFICATION AUTOMATION STUDY: AIDS 3
EVALUATION REPORT. VOLUME 9: FUNCTIONAL
REQUIREMENTS (Jet Propulsion Lab.) 48 p
HC A03/MF A01
CSCL 12/8 G3/66

N81-16834

Unclas
41231

FBI Fingerprint Identification Automation Study: AIDS III Evaluation Report

Volume IX: Functional Requirements

August 15, 1980

Prepared for
U.S. Department of Justice
Federal Bureau of Investigation
Through an agreement with
National Aeronautics and Space Administration
by
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

JPL PUBLICATION 80-79

FBI Fingerprint Identification Automation Study: AIDS III Evaluation Report

Volume IX: Functional Requirements

August 15, 1980

Prepared for
U.S. Department of Justice
Federal Bureau of Investigation
Through an agreement with
National Aeronautics and Space Administration
by
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

Prepared by the Jet Propulsion Laboratory, California Institute of Technology, and sponsored by the U.S. Department of Justice, Federal Bureau of Investigation, through an agreement with the National Aeronautics and Space Administration.

ABSTRACT

This volume, Functional Requirements, details the functional performance, and general requirements for the FBI Fingerprint Identification system. It will be used in evaluating the AIDS III system concept and the alternative systems that will be studied in the second phase of this work. The document describes the current system and subsystem used by the Identification Division. It also discusses system constraints that dictate the system environment and describes boundaries within which solutions must be found. The Functional Requirements section discusses the functional requirements and relates them to the performance requirements. These performance requirements, listed in the Measure of Effectiveness Volume VIII, are then related to their applicable subsystems. The Interface Requirements section describes the flow of data, documents, or other pieces of information from one subsystem to another or from the external world into the identification system. Finally, the General Requirements section lists the requirements and design standards for a computer-based system. For a synopsis of this entire report see the Executive Summary in the Compendium (Volume I).

ACKNOWLEDGMENT

The following persons have contributed to the analysis described in this report and/or to the preparation of this report:

H. Alioth
E. Bahm
C. Beswick
C. Brunstein
P. Caples
R. Chafin
J. Chillemi
E. Cuddihy
R. Cunningham
J. Eskenazi
A. Feinberg
E. Gold
M. Goldberger
M. Gottdiener
D. Hopelain
J. Johnson
L. Keith
F. Kuhn
J. Lee
P. Lindley

W. MacFadden
R. Mancini
R. Miles
R. Miller
A. Mobilia
S. Mouneimne
J. Mustain
L. Perelman
C. Schober
D. Schwartz
C. Seafeldt
M. Slonski
E. Records
I. Reed
J. Urena
L. Webster
C. Weiner
R. Wells
J. Whitney

B. D. L. Mulhall
Task Manager

CONTENTS

APPENDIXES

Figures

SECTION I

INTRODUCTION

A. DEFINITIONS AND PURPOSE

There are four terms used extensively in this document which may not be familiar to the reader. These are:

(1) Functional requirements.

(2) Performance requirements.

(3) Top down functional analysis.

(4) Measures of effectiveness.

Functional requirements are the collection of the capabilities that a system and its subsystem must possess to fulfill the objectives of the users of the system. In other words, they are what the system needs to do to meet its intended purpose or reason for existence. The user requirements that are fulfilled are under the control of the operator and/or owner of the system. Functional requirements are not design characteristics. Rather, functional requirements indicate to the designer the capabilities that must be incorporated into the design.

Performance requirements describe the level of quality with which each function must be accomplished. Consequently, performance requirements are generally quantifiable and, as such, can be measured.

The determination of the functional requirements of a system can be accomplished in more than one way. An extremely effective method is top down functional analysis (TDFA). (See Volume VII for a TDFA of the FBI's Identification Division.) This method starts at the highest level objective and by asking the question, "what functions need to be performed to achieve this objective," a division into subfunctions is made. When the complete set of subfunctions supporting the function has been identified, each of the subfunctions is in turn subdivided until the lowest useful level is reached. Deciding when the lowest useful level has been reached is not easy. One test is that further subdivision requires design decisions. At this point, the process should stop.

Measures of effectiveness (MOE) are the parameters used to gauge the state and performance of a system in attempting to achieve its goals.

Measures of effectiveness were used as a source of performance requirements since performance requirements are a subset or an essential ingredient of the measures of effectiveness. The measures of effectiveness (See Volume VIII) are primarily intended for use in the second phase of the study and therefore are different in approach and in scope.

The purpose of this document is to collect and list the functional, performance, and general requirements for the FBI fingerprint identification system. The document will be used to evaluate the AIDS III system concept and the alternative systems to be studied in the second phase of the study (Reference 2).

This document can also be used as a system development tool for contracting for system design and implementation and as a basis for acceptance testing both at the system and subsystem levels.

B. SCOPE

All the functional, performance, interface, and other general requirements for the FBI Identification process are collected in this document. The document will be used primarily for the evaluation of Rockwell International's AIDS III design concept. This Phase I (Reference 2) evaluation will exclude the Mail Room at either end of the processing as well as the latent print identification. When Phase I is complete, alternative design concepts will be evaluated in a second phase. At that time, the scope of this document may be changed to include data collection in and beyond the Mail Room and the identification of latent prints.

C. METHODOLOGY

The development of functional requirements is illustrated in Figure 1-1. First a TDFA is performed. This analysis breaks the objectives and functions of the Identification Division into increasingly more detailed subfunctions until further breakdowns become so design dependent as to no longer be functional in nature. Functions that are candidates for automation are identified. Those functions that were automated by AIDS I and II are marked as well as those which are to be automated by AIDS III (Reference 1).

A functional design is then created that requires the identification of subsystems. Some design decisions are involved in this step but are minimized. Next, functional interfaces between subsystems are determined as well as function and major components such as data files.

In parallel with these steps, MOE are developed. The MOE are then related to the functional system design by correlating the MOE to the functions of the TDFA by subsystem.

The next step requires the involvement of the FBI since the designer cannot know the importance of accuracy of search, speed of response, etc., without consulting with the operators and sponsors of the system. After determining system level performance requirements, the system engineers can allocate these to the affected subsystem, which leads to a complete set of system and subsystem functional requirements. These requirements can be used to communicate to the

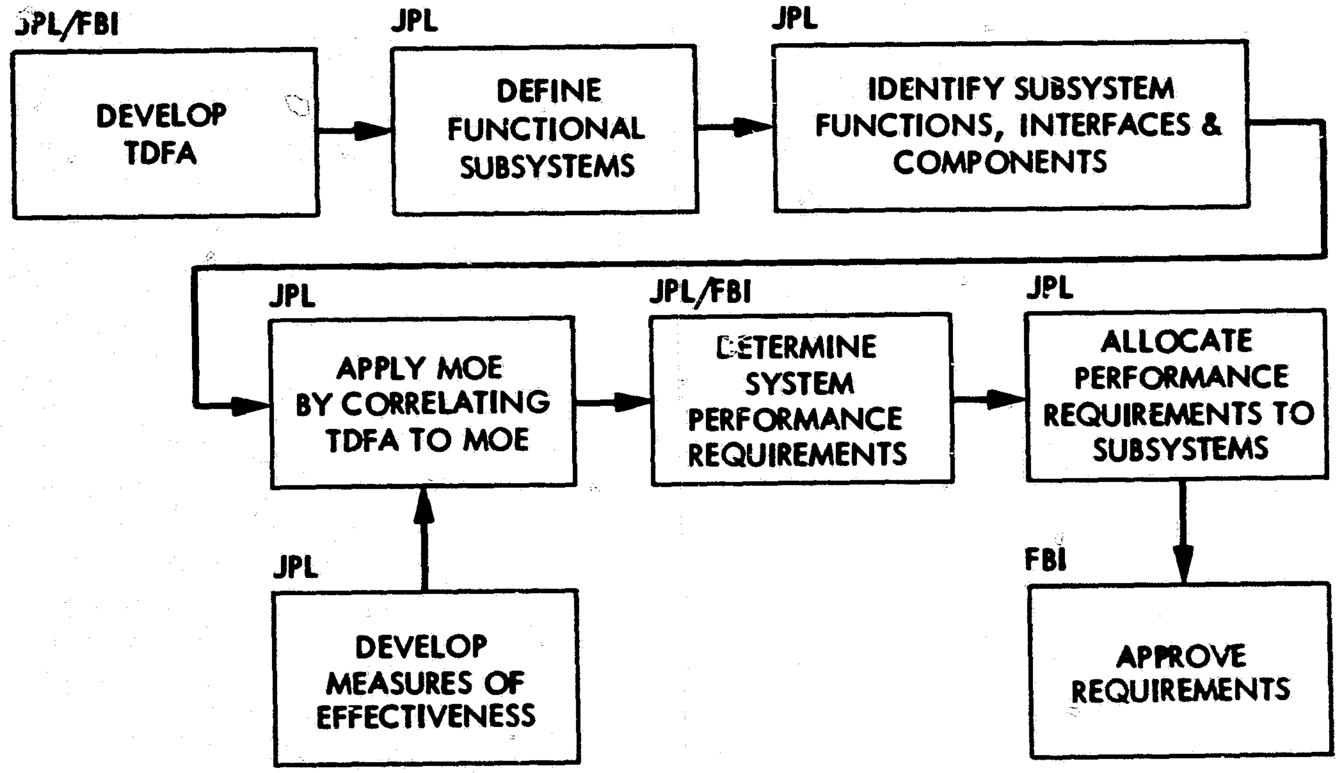

JPL/FBI
DEVELOP TDFA
JPL
DEFINE FUNCTIONAL SUBSYSTEMS
JPL
IDENTIFY SUBSYSTEM FUNCTIONS, INTERFACES & COMPONENTS
JPL
APPLY MOE BY CORRELATING TDFA TO MOE
JPL/FBI
DETERMINE SYSTEM PERFORMANCE REQUIREMENTS
JPL
ALLOCATE PERFORMANCE REQUIREMENTS TO SUBSYSTEMS
JPL
DEVELOP MEASURES OF EFFECTIVENESS
FBI
APPROVE REQUIREMENTS

Figure 1-1. Functional Requirements Development

builders of the system with the assurance that the system will perform the necessary functions, that all interfaces will be properly designed, and that the system will respond and perform as intended.

SECTION II

SYSTEM AND SUBSYSTEM DESCRIPTIONS

A. FINGERPRINT CARD AND EXTERNAL DOCUMENT FLOW

Figure 2-1 shows the flow of fingerprint cards and other external documents that are received by the FBI and processed through the Identification System. As discussed earlier, the scope of this document in Phase I is bounded by the Mail Room as the point of data collection and response disbursement.

The Data Collection Subsystem (see Figure 2-1) receives the requests from the Mail Room. Alien and identification cards are immediately sent to the civil file for storage. (Those documents that must be searched in Card Index are sent to the manual system.) In the Data Entry Subsystem incomplete requests are returned to the originating users and the data on the request documents are entered and verified.

The subject search is done first. A response is returned to the terminal operator. This response will indicate to the operator where the documents are to be routed. Military requests with no candidates from the subject search are not fingerprint (technical) searched and are sent to the civil file for storage. Documents that are to be returned to the user with no further processing are sent to the Response Generation Subsystem. The manual system can also be a source for the Data Entry Subsystem when a positive identification is made as a result of a search in the manual system. If the subject's file indicates that the records are in the automated subject file, that file must be updated with the new information.

Criminal and civil search requests with no tentative search candidates are sent to the Technical Search Subsystem. Search requests with search candidates go to the Identification/Verification (I/V) Subsystem for a positive identification. If a positive identification is not made in the I/V Subsystem, then these candidates are routed to the Technical Search Subsystem for further search.

In the fingerprint search all searches that produce no candidates are sent to the Response Generation Subsystem and those with candidates are sent to the I/V Subsystem. If no identification can be made, the document is sent to Response Generation for the appropriate response. If it is a criminal inquiry it also receives file updating. When a positive identification is made, the document will be sent to Response Generation for the response and file updates, or, if the FBI number indicates that the subject's file is in the manual system (Card Index), the request document will be routed to the manual system. If necessary, the Response Generation Subsystem will generate an index card that is also sent to the manual system to be filed in the Card Index files.

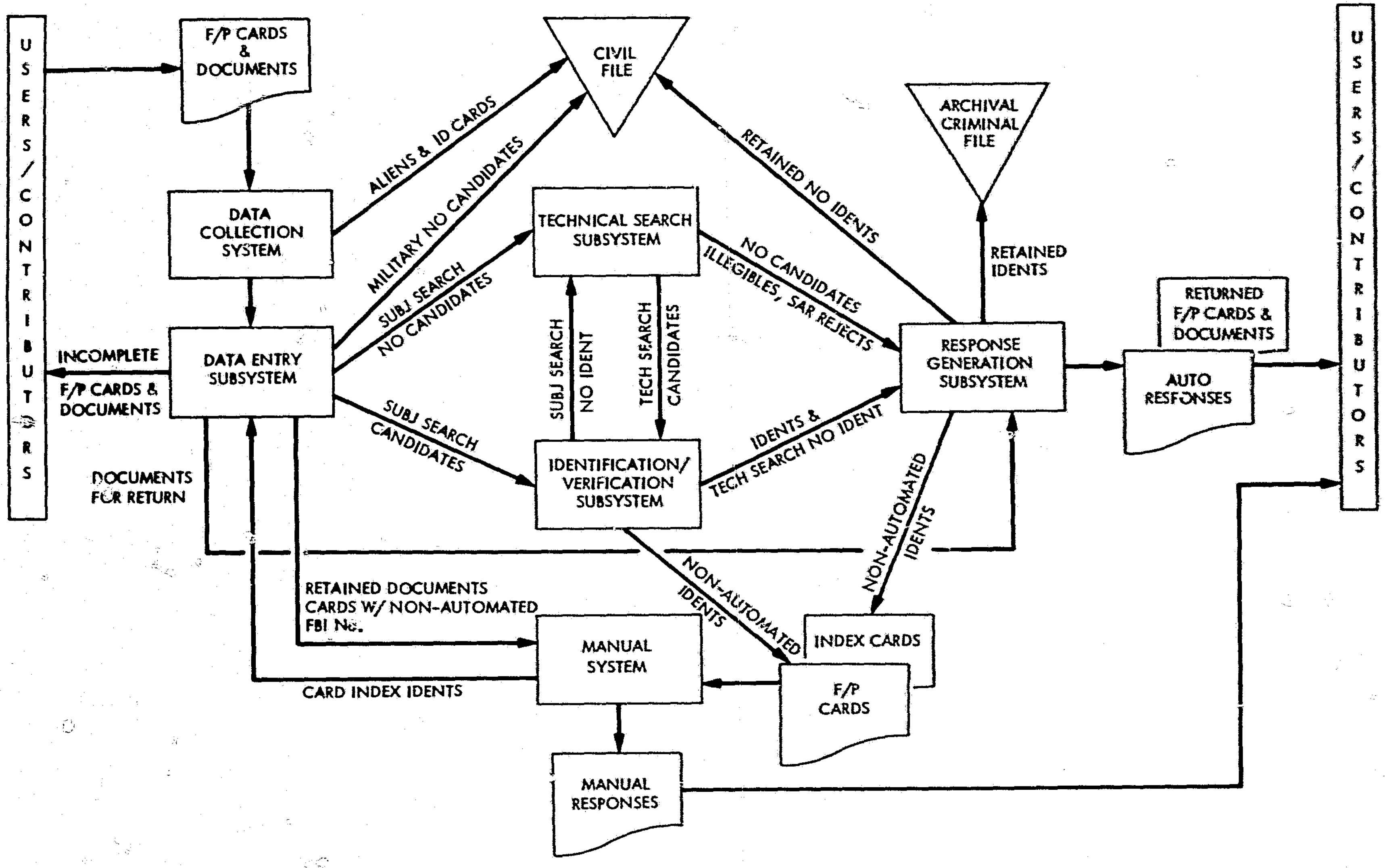


Figure 2-1. Fingerprint Card and External Document Flow

ORIGINAL PAGE IS OF POOR QUALITY

From the Response Generation Subsystem, retained documents are forwarded to either the Civil or the Archival Criminal File. Documents to be returned and responses are sent to the contributors.

B. SYSTEM DATA FLOW

Figure 2-2 shows the logical data interfaces between the functional subsystems in the Identification System.

Data is received from the users and contributors in the external world by the Data Collection Subsystem. In the Data Entry Subsystem this data is converted into machine-readable characters in appropriate formats for that kind of data; i.e. search requests, dispositions, etc.

The System Supervisor serves as a control interface between the subsystems to monitor and control the transactions as they pass through the system. The data are made available directly to the appropriate subsystem for processing.

Pointers to the data are passed through the System Supervisor. For example, in the case of a search request, a control record is generated indicating that the Subject Search Subsystem is processing a specific process control number (PCN). The record contains other information such as date and time of release to the subsystem and the type and source of the transaction for audit trail and statistical reporting. When processing is completed in the Subject Search, the response (either a candidate or no candidate indication) is passed back to the Data Entry terminal operator through the System Supervisor. The list of candidates, if any, is made directly available to the operator.

The automated responses are generated by accessing the Subject Data File and are distributed to the users. Figure 2-2 also indicates the responsibilities and relationships of subsystems and each of the major master files in the system.

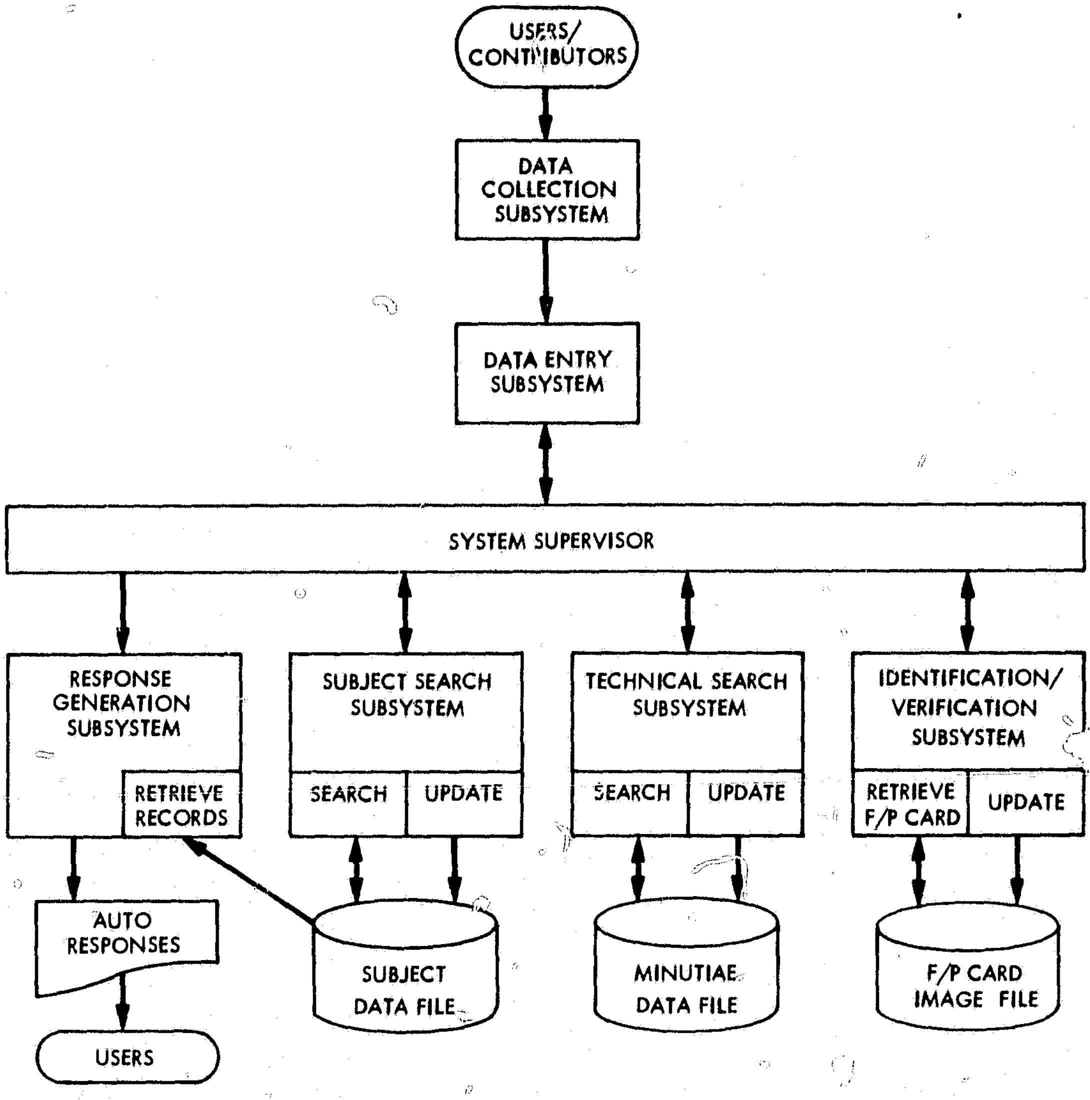


Figure 2-2. System Data Flow

SECTION III

SYSTEM CONSTRAINTS

The objectives[1] that are externally imposed and thus dictate the system environment are system constraints. They define the boundaries of a solution space within which a technically, operationally, and economically feasible solution must be found in order to establish system feasibility.

The objectives, which are constraints as opposed to requirements (which are listed in Section IV), can be paraphrased as follows:

(1) Automation should not require personnel to work hours different from those already established for the manual system. The maximum daily work loads should be processed in the two 7.5-hour shifts that are staffed at a ratio of 2 to 1, day shift to night shift.

(2) Implementation of automation must occur within the work space alloted to the Identification Division. No consideration can be given to adding floors to the J. Edgar Hoover Building nor to moving to a new building to accommodate automation.

(3) Processing the work by automated procedures should not require a change in the size of the fingerprint card form nor a change in the information contained on it. Manual forms now in use must be processed in the automated system.

(4) Daily work loads must be satisfied using the five existing automatic Fingerprint Reader Systems (AFRS).

[1] Stated in the Appendix of "Automation of FBI Identification Functions: Feasibility Study Work Requirements Statement," unnumbered document, Federal Bureau of Investigation, Technical Services Division, May 22, 1979.

SECTION IV

FUNCTIONAL REQUIREMENTS

This section lists the system and subsystem functional requirements. Functional requirements are purely qualitative in nature as opposed to performance requirements (see Section V), which may be qualitative or quantitative.

The functions for the system and for each subsystem are shown in Figures 4-1 through 4-9, which also show functional interfaces.

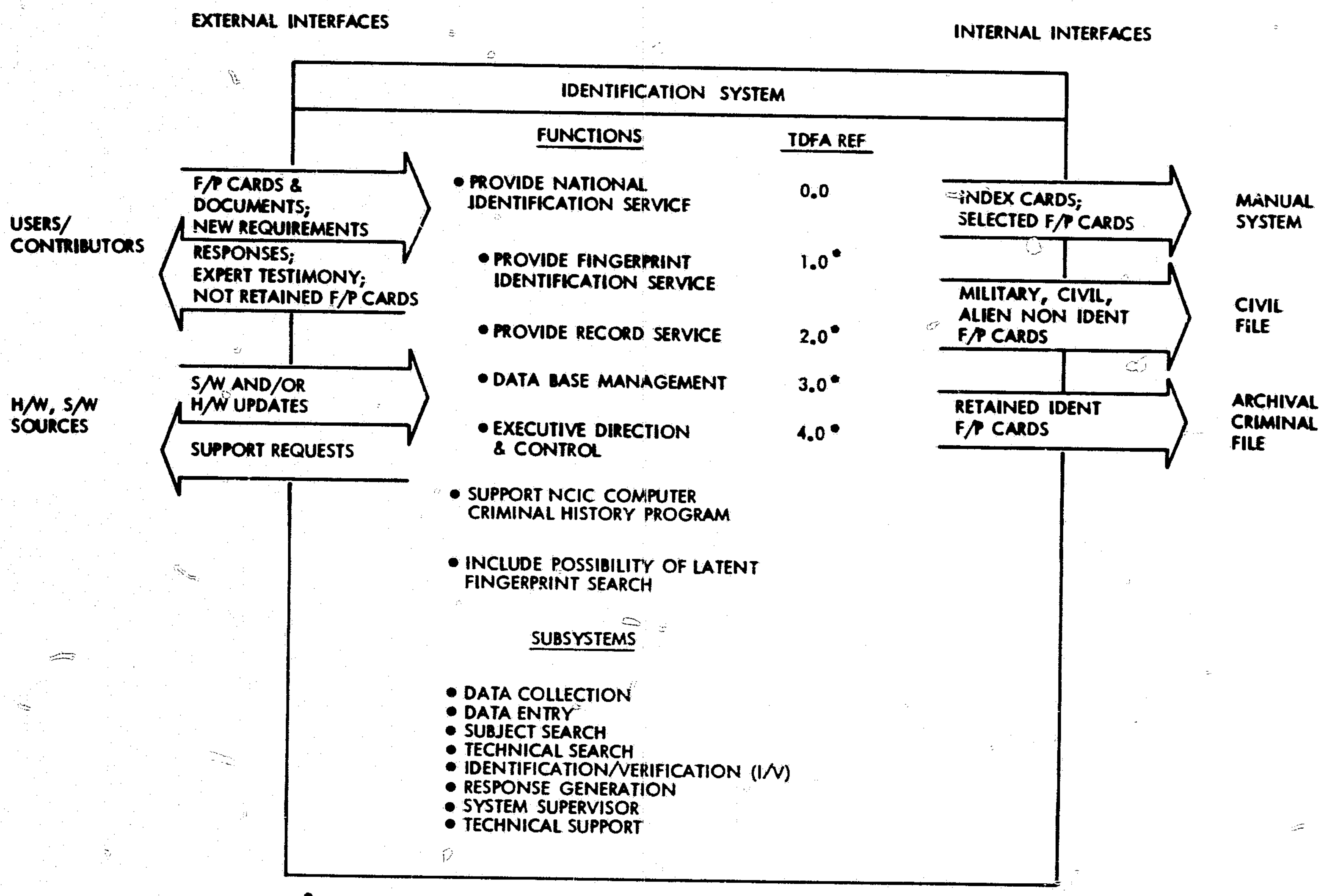
A. SYSTEM

Figure 4-1 shows the functions from the TDFA of the Identification System. Listed on the chart are the subsystems that comprise the system and the major external interfaces, other systems, and files within the FBI that lie outside the scope of this document.

B. SUBSYSTEMS

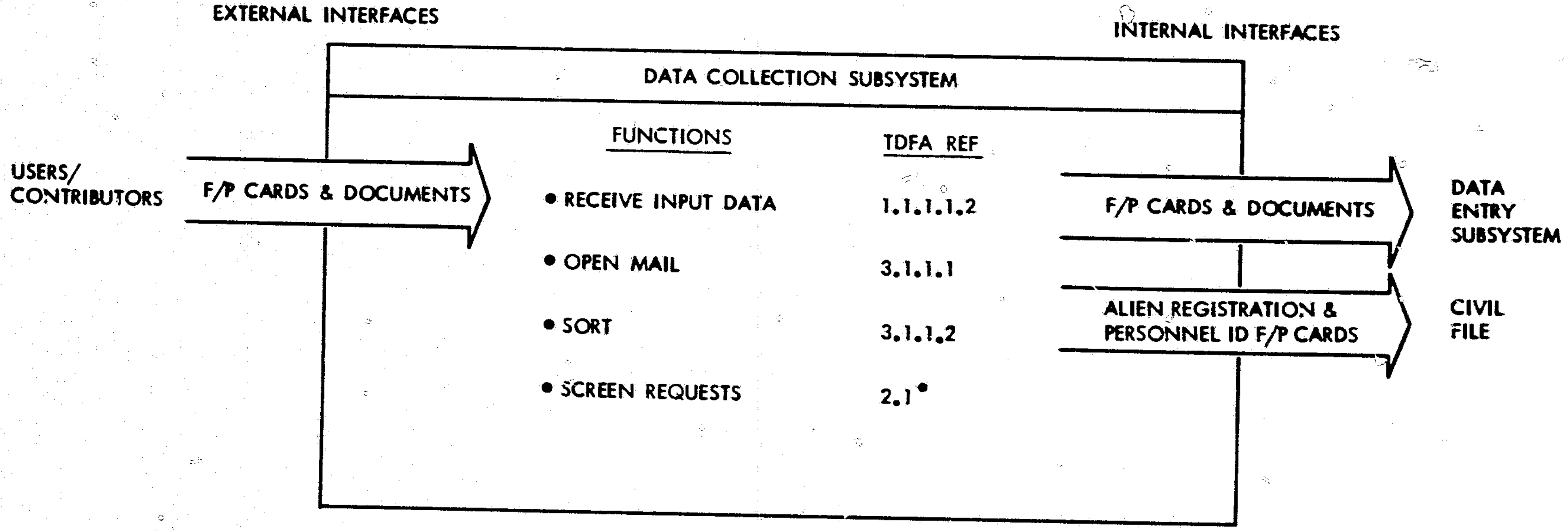
Figures 4-2 through 4-9 show the TDFA functions performed by each of the subsystems listed in Figure 4-1. These charts list major data files included in the subsystem and the major interfaces to other subsystems. Different interfaces are listed on each side of the chart with the appropriate heading. In most cases, the interfaces are either functional (data) or physical (fingerprint cards). Where the subsystem deals with the external world, the external and internal interfaces are on opposite sides of the chart. If there are only functional interfaces, these were divided in a manner that would facilitate the reader's understanding of the data flow. These headings are important to the interpretation of the charts.

The functions listed within each chart are only the highest applicable level listed in the TDFA. The reader is referred to the TDFA (Reference 1) for the breakdown of these functions into their components.



• SUBFUNCTIONS LISTED IN TDFA

Figure 4-1. Identification System Functional Requirements



* SUBFUNCTIONS LISTED IN TDFA

Figure 4-2. Data Collection Subsystem

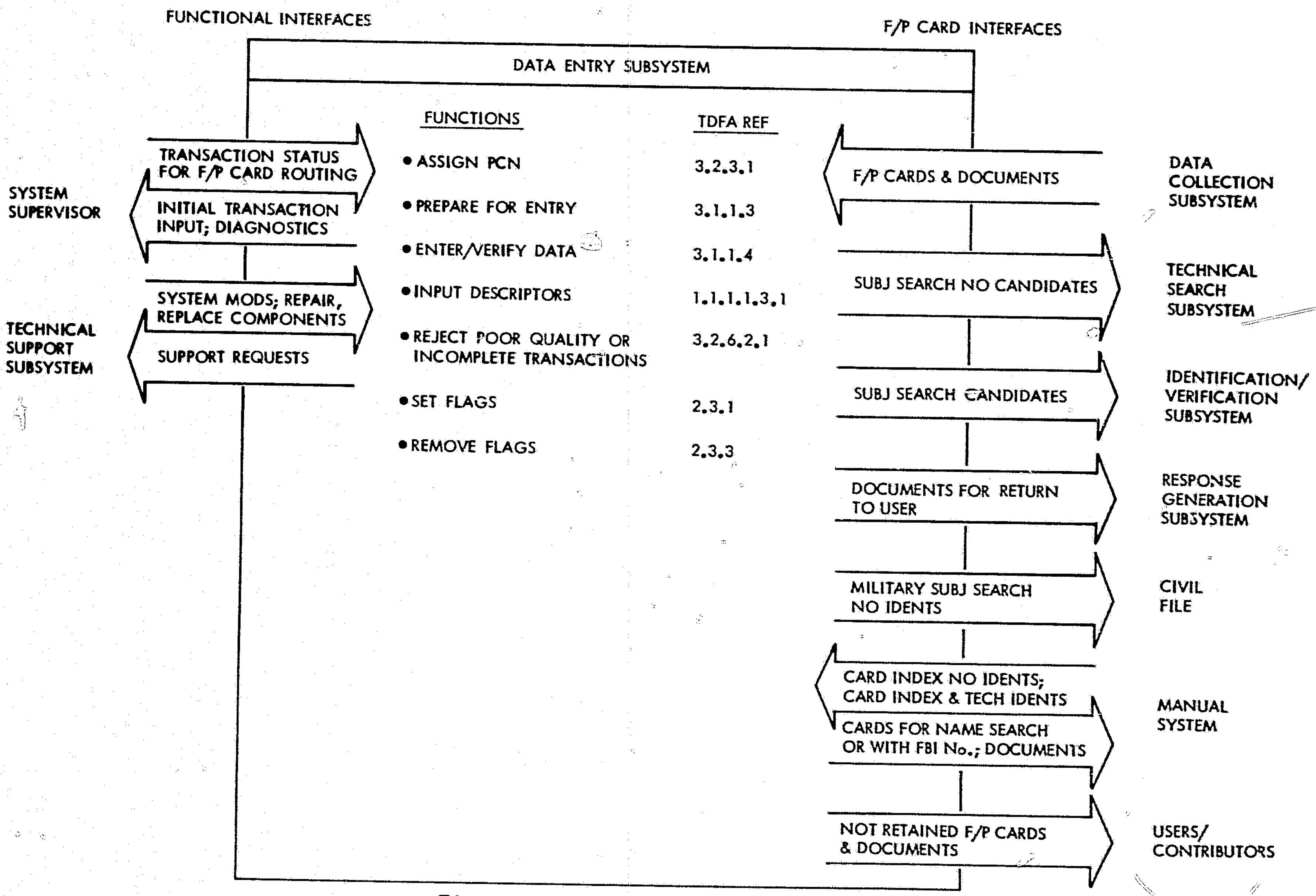

FUNCTIONAL INTERFACES
F/P CARD INTERFACES
DATA ENTRY SUBSYSTEM
FUNCTIONS
TDFA REF
• ASSIGN PCN
3.2.3.1
• PREPARE FOR ENTRY
3.1.1.3
• ENTER/VERIFY DATA
3.1.1.4
• INPUT DESCRIPTORS
1.1.1.1.3.1
• REJECT POOR QUALITY OR INCOMPLETE TRANSACTIONS
3.2.6.2.1
• SET FLAGS
2.3.1
• REMOVE FLAGS
2.3.3
SYSTEM SUPERVISOR
TRANSACTION STATUS FOR F/P CARD ROUTING
INITIAL TRANSACTION INPUT; DIAGNOSTICS
TECHNICAL SUPPORT SUBSYSTEM
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS
F/P CARDS & DOCUMENTS
DATA COLLECTION SUBSYSTEM
SUBJ SEARCH NO CANDIDATES
TECHNICAL SEARCH SUBSYSTEM
SUBJ SEARCH CANDIDATES
IDENTIFICATION/ VERIFICATION SUBSYSTEM
DOCUMENTS FOR RETURN TO USER
RESPONSE GENERATION SUBSYSTEM
MILITARY SUBJ SEARCH NO IDENTS
CIVIL FILE
CARD INDEX NO IDENTS; CARD INDEX & TECH IDENTS
CARDS FOR NAME SEARCH OR WITH FBI No.; DOCUMENTS
MANUAL SYSTEM
NOT RETAINED F/P CARDS & DOCUMENTS
USERS/ CONTRIBUTORS

Figure 4-3. Data Entry Subsystem

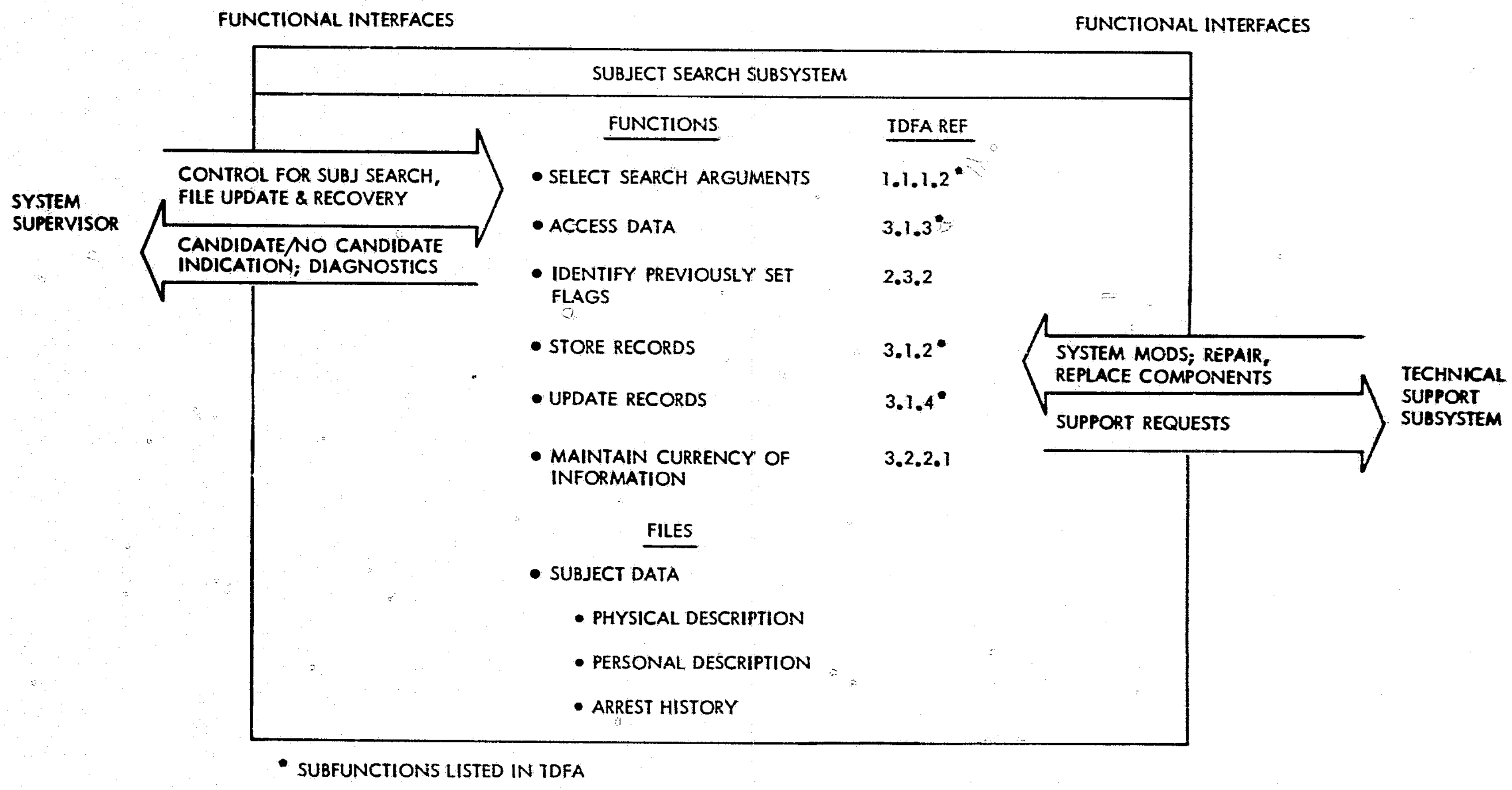

FUNCTIONAL INTERFACES
FUNCTIONAL INTERFACES
SUBJECT SEARCH SUBSYSTEM
SYSTEM SUPERVISOR
CONTROL FOR SUBJ SEARCH, FILE UPDATE & RECOVERY
CANDIDATE/NO CANDIDATE INDICATION; DIAGNOSTICS
FUNCTIONS
TDFA REF
• SELECT SEARCH ARGUMENTS
1.1.1.2*
• ACCESS DATA
3.1.3*
• IDENTIFY PREVIOUSLY SET FLAGS
2.3.2
• STORE RECORDS
3.1.2*
• UPDATE RECORDS
3.1.4*
• MAINTAIN CURRENCY OF INFORMATION
3.2.2.1
FILES
• SUBJECT DATA
• PHYSICAL DESCRIPTION
• PERSONAL DESCRIPTION
• ARREST HISTORY
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS
TECHNICAL SUPPORT SUBSYSTEM
* SUBFUNCTIONS LISTED IN TDFA

Figure 4-4. Subject Search Subsystem

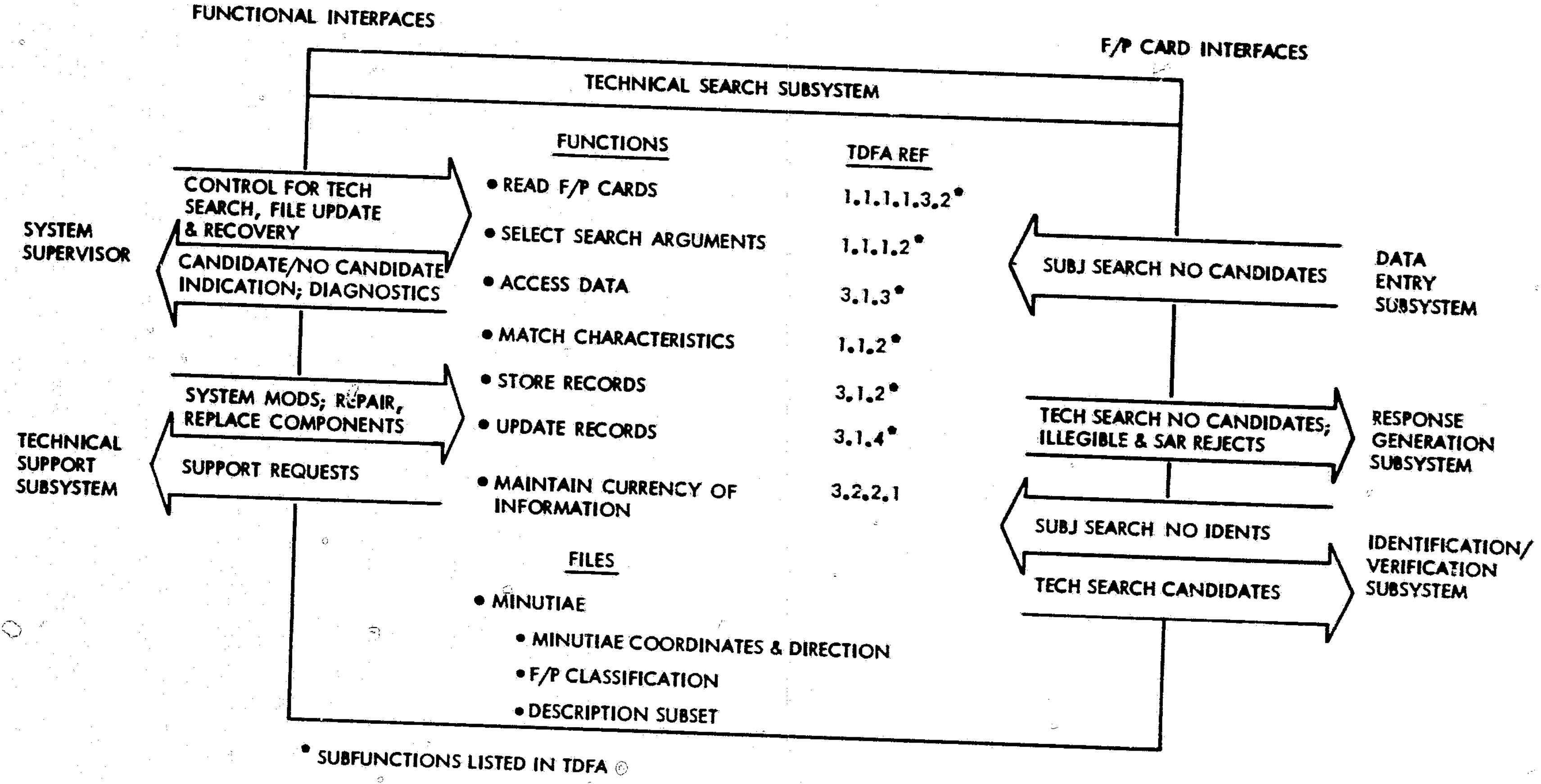
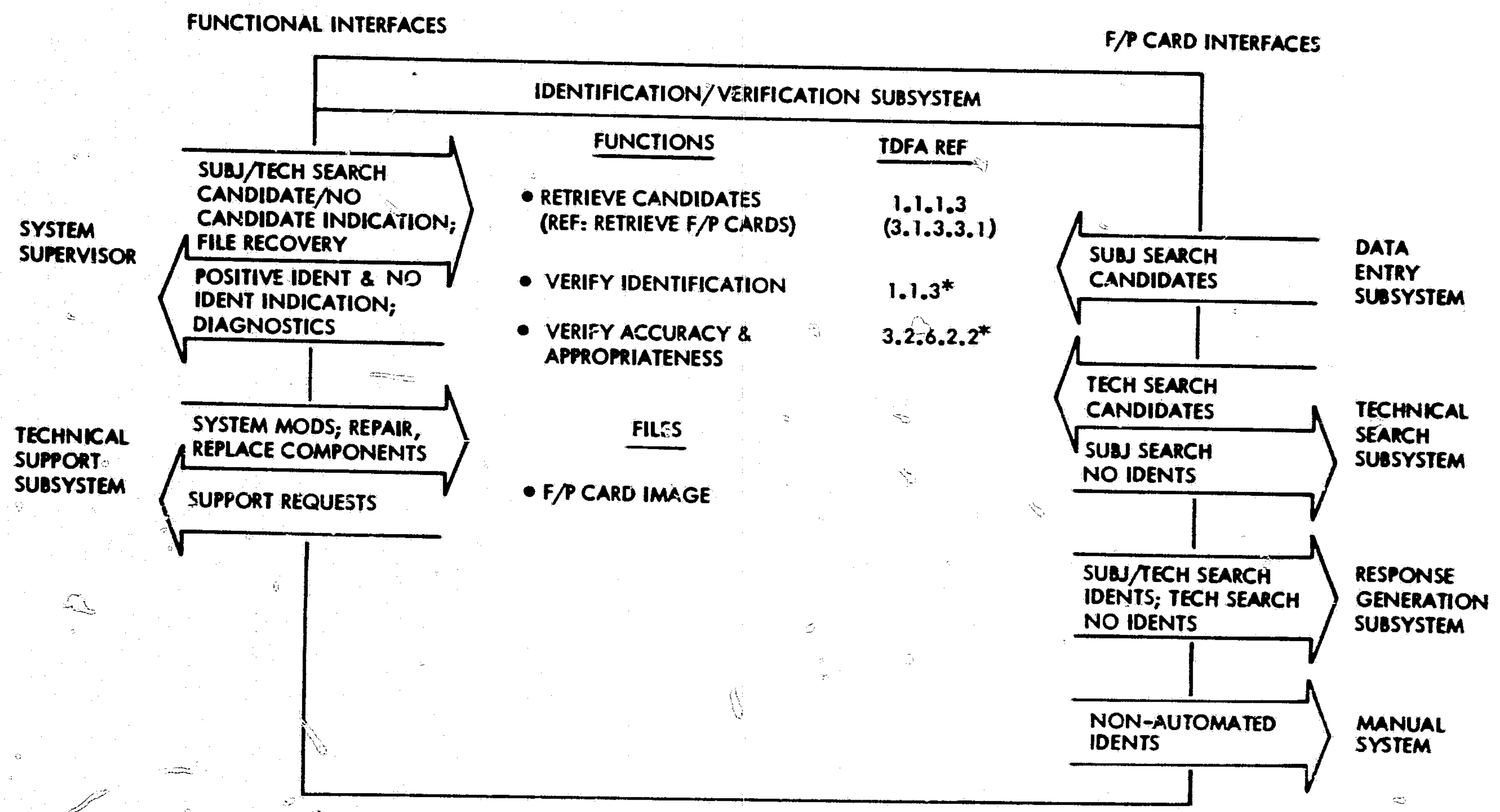
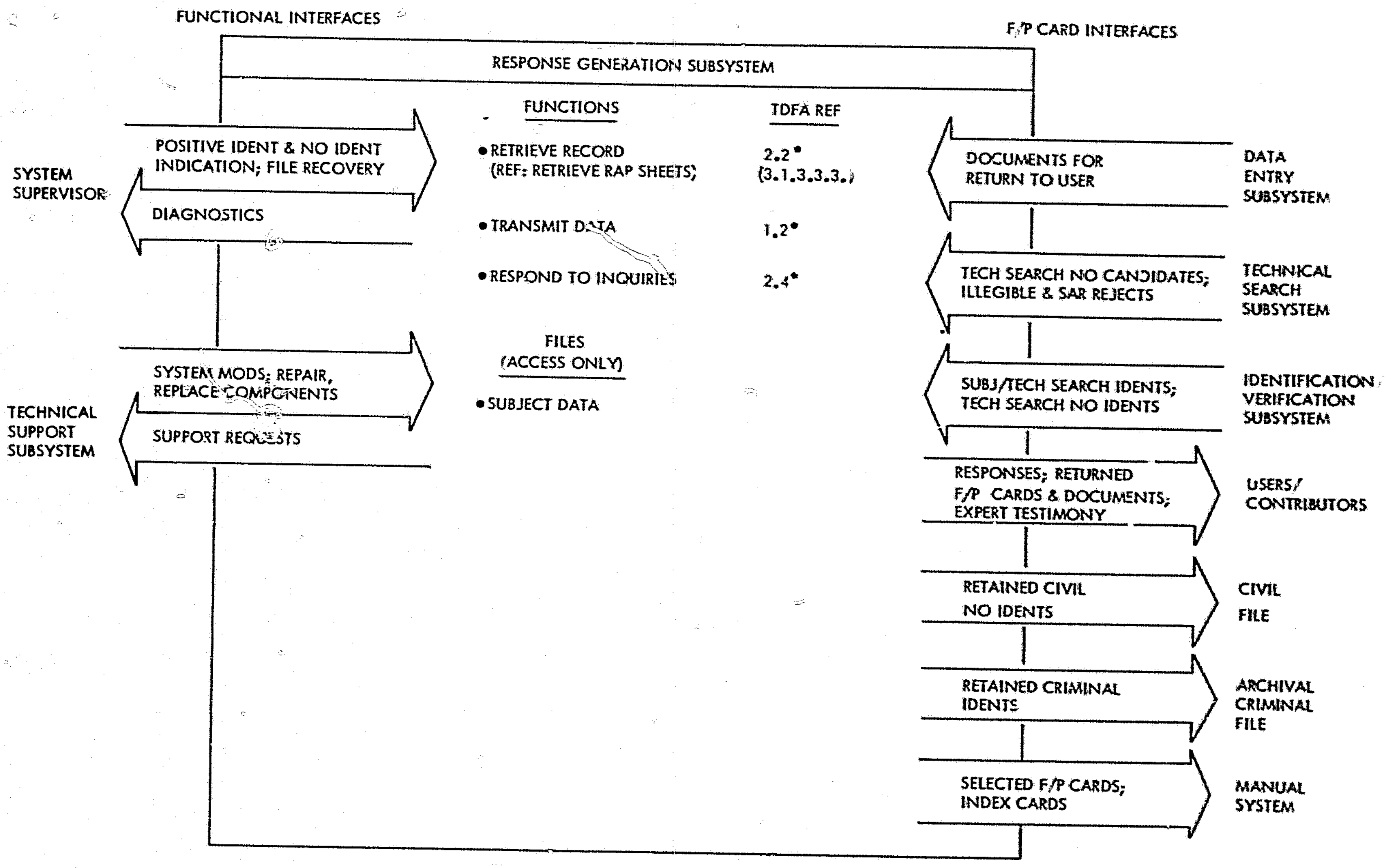

FUNCTIONAL INTERFACES
F/P CARD INTERFACES
TECHNICAL SEARCH SUBSYSTEM
FUNCTIONS
TDFA REF
• READ F/P CARDS
1.1.1.1.3.2*
• SELECT SEARCH ARGUMENTS
1.1.1.2*
• ACCESS DATA
3.1.3*
• MATCH CHARACTERISTICS
1.1.2*
• STORE RECORDS
3.1.2*
• UPDATE RECORDS
3.1.4*
• MAINTAIN CURRENCY OF INFORMATION
3.2.2.1
FILES
• MINUTIAE
• MINUTIAE COORDINATES & DIRECTION
• F/P CLASSIFICATION
• DESCRIPTION SUBSET
* SUBFUNCTIONS LISTED IN TDFA
SYSTEM SUPERVISOR
CONTROL FOR TECH SEARCH, FILE UPDATE & RECOVERY
CANDIDATE/NO CANDIDATE INDICATION; DIAGNOSTICS
TECHNICAL SUPPORT SUBSYSTEM
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS
DATA ENTRY SUBSYSTEM
SUBJ SEARCH NO CANDIDATES
RESPONSE GENERATION SUBSYSTEM
TECH SEARCH NO CANDIDATES; ILLEGIBLE & SAR REJECTS
IDENTIFICATION/ VERIFICATION SUBSYSTEM
SUBJ SEARCH NO IDENTS
TECH SEARCH CANDIDATES

Figure 4-5. Technical Search Subsystem


FUNCTIONAL INTERFACES
F/P CARD INTERFACES
IDENTIFICATION/VERIFICATION SUBSYSTEM
FUNCTIONS
TDFA REF
● RETRIEVE CANDIDATES (REF: RETRIEVE F/P CARDS)
1.1.1.3 (3.1.3.3.1)
● VERIFY IDENTIFICATION
1.1.3*
● VERIFY ACCURACY & APPROPRIATENESS
3.2.6.2.2*
FILES
● F/P CARD IMAGE
SYSTEM SUPERVISOR
SUBJ/TECH SEARCH CANDIDATE/NO CANDIDATE INDICATION; FILE RECOVERY
POSITIVE IDENT & NO IDENT INDICATION; DIAGNOSTICS
TECHNICAL SUPPORT SUBSYSTEM
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS
DATA ENTRY SUBSYSTEM
SUBJ SEARCH CANDIDATES
TECHNICAL SEARCH SUBSYSTEM
TECH SEARCH CANDIDATES
SUBJ SEARCH NO IDENTS
RESPONSE GENERATION SUBSYSTEM
SUBJ/TECH SEARCH IDENTS; TECH SEARCH NO IDENTS
MANUAL SYSTEM
NON-AUTOMATED IDENTS

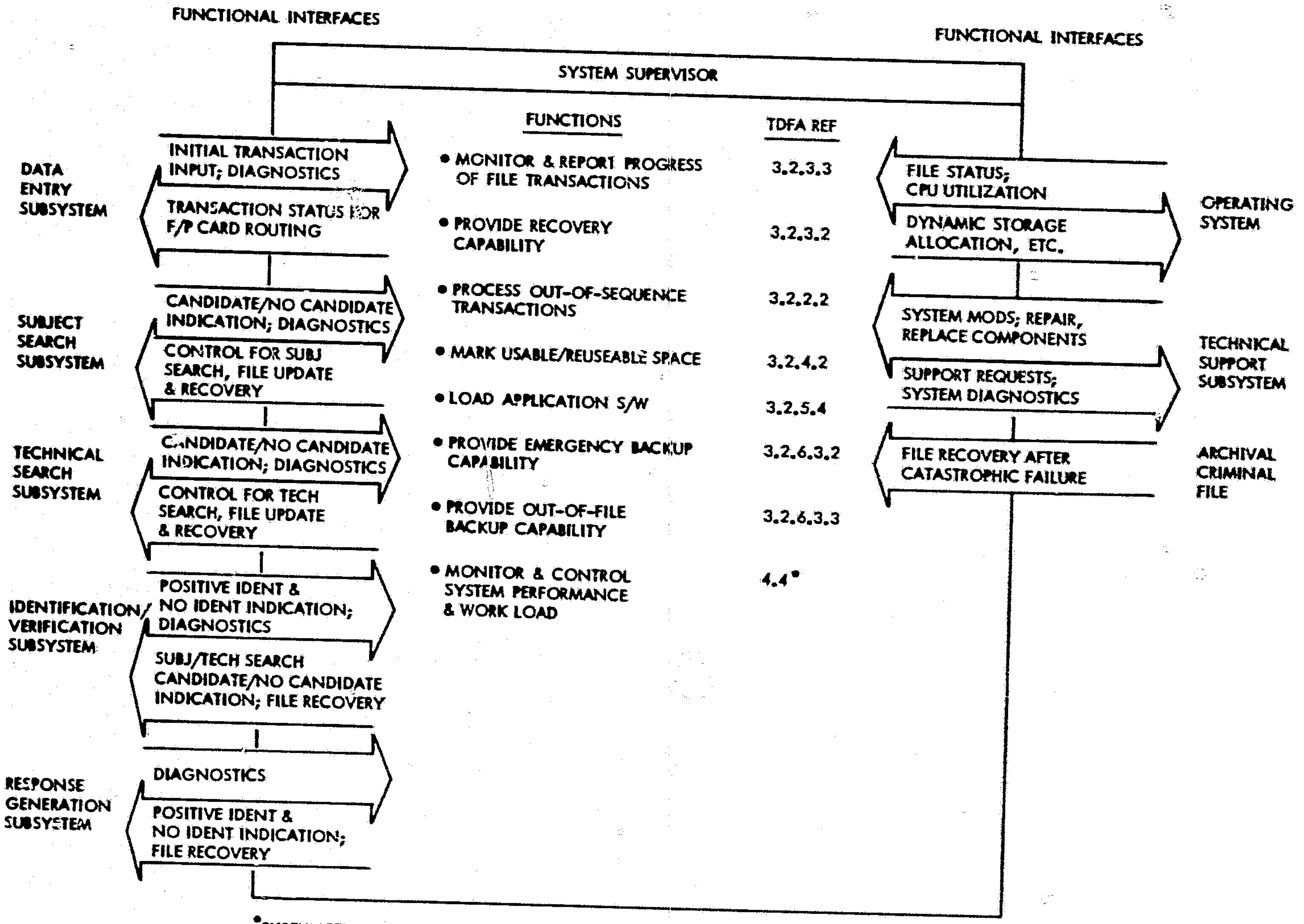
*SUBFUNCTIONS LISTED IN TDFA

Figure 4-6. Identification/Verification Subsystem


FUNCTIONAL INTERFACES
F/P CARD INTERFACES
RESPONSE GENERATION SUBSYSTEM
FUNCTIONS
TDFA REF
●RETRIEVE RECORD (REF: RETRIEVE RAP SHEETS)
2.2* (3.1.3.3.3.)
●TRANSMIT DATA
1.2*
●RESPOND TO INQUIRIES
2.4*
FILES (ACCESS ONLY)
●SUBJECT DATA
SYSTEM SUPERVISOR
POSITIVE IDENT & NO IDENT INDICATION; FILE RECOVERY
DIAGNOSTICS
TECHNICAL SUPPORT SUBSYSTEM
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS
DATA ENTRY SUBSYSTEM
DOCUMENTS FOR RETURN TO USER
TECHNICAL SEARCH SUBSYSTEM
TECH SEARCH NO CANDIDATES; ILLEGIBLE & SAR REJECTS
IDENTIFICATION VERIFICATION SUBSYSTEM
SUBJ/TECH SEARCH IDENTS; TECH SEARCH NO IDENTS
USERS/ CONTRIBUTORS
RESPONSES; RETURNED F/P CARDS & DOCUMENTS; EXPERT TESTIMONY
CIVIL FILE
RETAINED CIVIL NO IDENTS
ARCHIVAL CRIMINAL FILE
RETAINED CRIMINAL IDENTS
MANUAL SYSTEM
SELECTED F/P CARDS; INDEX CARDS

*SUBFUNCTIONS LISTED IN TDFA

Figure 4-7. Response Generation Subsystem


FUNCTIONAL INTERFACES
FUNCTIONAL INTERFACES
SYSTEM SUPERVISOR
FUNCTIONS
TDFA REF
• MONITOR & REPORT PROGRESS OF FILE TRANSACTIONS
3.2.3.3
• PROVIDE RECOVERY CAPABILITY
3.2.3.2
• PROCESS OUT-OF-SEQUENCE TRANSACTIONS
3.2.2.2
• MARK USABLE/REUSEABLE SPACE
3.2.4.2
• LOAD APPLICATION S/W
3.2.5.4
• PROVIDE EMERGENCY BACKUP CAPABILITY
3.2.6.3.2
• PROVIDE OUT-OF-FILE BACKUP CAPABILITY
3.2.6.3.3
• MONITOR & CONTROL SYSTEM PERFORMANCE & WORK LOAD
4.4*
DATA ENTRY SUBSYSTEM
INITIAL TRANSACTION INPUT; DIAGNOSTICS
TRANSACTION STATUS FOR F/P CARD ROUTING
SUBJECT SEARCH SUBSYSTEM
CANDIDATE/NO CANDIDATE INDICATION; DIAGNOSTICS
CONTROL FOR SUBJ SEARCH, FILE UPDATE & RECOVERY
TECHNICAL SEARCH SUBSYSTEM
CANDIDATE/NO CANDIDATE INDICATION; DIAGNOSTICS
CONTROL FOR TECH SEARCH, FILE UPDATE & RECOVERY
IDENTIFICATION/ VERIFICATION SUBSYSTEM
POSITIVE IDENT & NO IDENT INDICATION; DIAGNOSTICS
SUBJ/TECH SEARCH CANDIDATE/NO CANDIDATE INDICATION; FILE RECOVERY
RESPONSE GENERATION SUBSYSTEM
DIAGNOSTICS
POSITIVE IDENT & NO IDENT INDICATION; FILE RECOVERY
OPERATING SYSTEM
FILE STATUS; CPU UTILIZATION
DYNAMIC STORAGE ALLOCATION, ETC.
TECHNICAL SUPPORT SUBSYSTEM
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SUPPORT REQUESTS; SYSTEM DIAGNOSTICS
ARCHIVAL CRIMINAL FILE
FILE RECOVERY AFTER CATASTROPHIC FAILURE

*SUBFUNCTIONS LISTED IN TDFA

Figure 4-8. System Supervisor

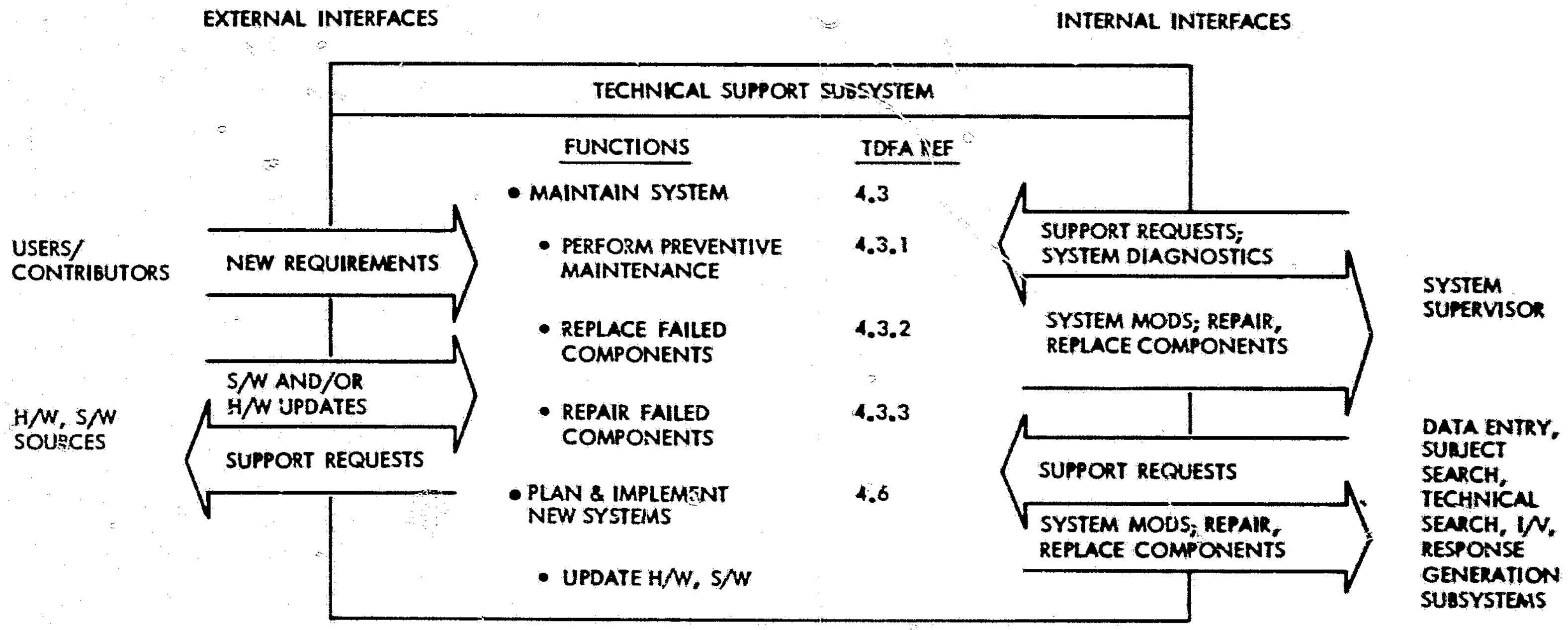

EXTERNAL INTERFACES
INTERNAL INTERFACES
TECHNICAL SUPPORT SUBSYSTEM
FUNCTIONS
TDFA REF
• MAINTAIN SYSTEM
4.3
• PERFORM PREVENTIVE MAINTENANCE
4.3.1
• REPLACE FAILED COMPONENTS
4.3.2
• REPAIR FAILED COMPONENTS
4.3.3
• PLAN & IMPLEMENT NEW SYSTEMS
4.6
• UPDATE H/W, S/W
USERS/ CONTRIBUTORS
NEW REQUIREMENTS
H/W, S/W SOURCES
S/W AND/OR H/W UPDATES
SUPPORT REQUESTS
SUPPORT REQUESTS; SYSTEM DIAGNOSTICS
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
SYSTEM SUPERVISOR
SUPPORT REQUESTS
SYSTEM MODS; REPAIR, REPLACE COMPONENTS
DATA ENTRY, SUBJECT SEARCH, TECHNICAL SEARCH, I/V, RESPONSE GENERATION SUBSYSTEMS

Figure 4-9. Technical Support Subsystem

SECTION V

PERFORMANCE REQUIREMENTS

This section lists and describes the system performance requirements and, where possible, relates them to the subsystems. Of the 10 performance requirements, five are quantifiable and can be allocated among subsystems and five are not quantifiable.

Quantifiable performance requirements are:

(1) Average response time.

(2) Maximum response time.

(3) Storage capacity.

(4) Availability (including reliability).

(5) Accuracy.

Qualitative performance requirements are:

(1) Observability.

(2) Operability.

(3) Maintainability.

(4) Integrity.

(5) Security.

The first three performance requirements (see Figure 5-1) -- average and maximum response time and capacity, especially storage capacity -- are interrelated because they deal with the problem of how much data must be held by the system and by each subsystem at any one time. How rapidly the data must move both in terms of the average processing time and the longest allowable time for any transaction are grouped together because of this storage interrelationship.

(1) Average response time -- The average time at which work has to be processed through the system. If queues of work that cannot be processed by the next station are defined to exist in the subsystem that has just produced them or the one that is about to accept them, then the System Supervisor only passes control and file pointer information that is not in the pipeline of the process. Response time can be affected if queues build for the System Supervisor to perform the message switching. Consequently, the System Supervisor will receive allocation of average response time.

SUBSYSTEM	RESPONSE TIME MAXIMUM	 AVERAGE	CAPACITY PERMANENT (in millions of records)	 TEMPORARY[a] (in thousands of transactions)	 AVAILABILITY	 FILE UPDATE	ACCURACY SEARCH & MATCH	 IDENTIFICATION
DATA COLLECTION	NOTE 1[b]	NOTE 1[b]	N/A	N/A	NOTE 3[b]	N/A	N/A	N/A
DATA ENTRY	↓	↓	N/A	N/A	↓	NOTE 4[b]	NOTE 4[b]	↓
SUBJECT SEARCH	↓	↓	14.3	26.609	↓	N/A	↓	↓
TECHNICAL SEARCH	↓	↓	14-26	15.147	↓	↓	↓	N/A
IDENTIFICATION/ VERIFICATION	↓	↓	14-26	6.977	↓	↓	NOTE 4[b]	1.0
RESPONSE GENERATION	↓	↓	N/A	N/A	↓	↓	N/A	N/A
SYSTEM SUPERVISOR	NOTE 1[b]	NOTE 1[b]	NOTE 2[b]	42.042	NOTE 3[b]	N/A	N/A	N/A

N/A = NOT APPLICABLE

[a] DAILY AVERAGE FROM DESIGN GUIDELINE WORK LOAD FOR FINGERPRINT IDENTIFICATION FUNCTION

[b] SEE ACCOMPANYING TEXT

NOTE 1 & 2 ARE ON PAGE 5-3

NOTE 3 & 4 ARE ON PAGE 5-4

ORIGINAL PAGE IS
OF POOR QUALITY

Figure 5-1. Allocation of Performance Requirements

(2) Maximum response time -- The maximum allowable time that any one piece of work can dwell in the system prior to completion of processing. This maximum allowable time is normally associated with some probability since there is always the possibility of an unforeseen set of conditions or transactions that will, however rarely, exceed the specified response time.

Note 1. The FBI AIDS III Design Guidelines[2] require that the response time will be 8 work-hours (for routine) or 30 minutes (for expedite) for 95% of the fingerprint cards; 48 hours (routine) or 8 hours (expedite) for 99% of the cards, and 96 hours (routine) for 99.9% of the fingerprint cards. This performance requirement may be too stringent, but it has been agreed between JPL and the Identification Division that this and the other requirements will stand until it is shown that no operationally feasible solution exists within the solution space. At that time, the Identification Division will relax these boundaries. This solves the problem for Phase 1 of the JPL study. A more substantial solution will be sought for the evaluation of the alternative systems in the second phase.

(3) Permanent storage capacity -- Applies to file size and therefore is allocated to those subsystems that manage data files; i.e., Subject Search, Technical Search, and the Identification/Verification Subsystems. The estimated file sizes for AIDS III were defined in the AIDS III Design Guidelines.

(4) Temporary storage capacity -- Refers to the amount of data that must be handled concurrently or the work load that the subsystems must process in a period of time. The specific requirements for each subsystem are derived from the projected design work load requirements defined by the FBI.[2]

Note 2. The System Supervisor is allocated permanent and temporary storage capacity so that the data are available for work load monitoring and controlling and statistical reporting required of current or historical data in an interactive or batch mode.

The two remaining quantifiable requirements are:

(5) Availability including reliability -- Ratio of up to total time of required system operation. Total time is equal to up time plus down time. Down time consists of the time to

[2] "AIDS III Design Guidelines," attachment to letter from N. F. Stames, Assistant Director, Identification Division, Federal Bureau of Investigation, to R. E. Hilderbrand, Rockwell International, October 26, 1979.

detect a failure, the time to isolate, repair (including maintenance personnel travel), and to restore service.

Note 3. The availability requirements for the subsystem hardware is based upon the data in an AIDS III Technical Memo from Rockwell.[3]

(6) Accuracy -- Refers to the accuracy of searching, identifying, and updating files. This performance requirement applies to only four subsystems: Data Entry, Subject Search, Technical Search, and Identification/ Verification. Accuracy can be subdivided into three major categories: accuracy of the data entered for file update; searching and matching on the basis of descriptive information or fingerprints, which includes keying in the search data and such other functions as classification of fingerprints; and the final identification process, which produces only one identification or no identification. (See Figure 5-2.)

Note 4. It has been established that the allowable miss rate for false or wrong identifications is zero (accuracy probability required for identification is 1.0). In order to maintain a file from which no false identification can be made, the accuracy of the file update procedure must not allow any erroneous data to enter the file. This applies only to the conversion of data from the source document to the file; it does not apply to processes taking place outside the scope of this document. There is, however, an allowable miss rate for missed identifications. This can occur in the Data Entry, Subject Search, Technical Search, or Identification/Verification Subsystems. For the purpose of Phase 1 of the JPL study, the requirement will be that the new system must perform better than the existing manual system in making identifications. This performance level is documented in AIDS III Evaluation Report, Volume V: Current System Evaluation (Reference 3). This level of accuracy may need quantifying on an absolute scale for the evaluation of alternatives.

The remaining requirements are not quantifiable and therefore cannot be allocated to subsystems (see Figure 5-3):

(1) Observability -- The ability to monitor the performance of the system and detect surges or imbalances in work load as well as failures.

(2) Operability -- The ability to operate the system and the ease with which it can be operated both in normal and unusual circumstances.

[3] "AIDS III Technical Memo: Major Component MTBF/MTTR Summary and Availability Design Goal," by R. E. Davis, Rockwell International, November 12, 1979.

(4) Integrity -- Applies chiefly to data and includes the provisions for not corrupting or losing data.

(5) Security -- Involves the physical security of the system and its ability to prevent unauthorized access to or alteration of the information stored or in the process of flowing through the system.

ACCURACY	DATA ENTRY	SUBJECT SEARCH	TECH SEARCH	I/V
FILE UPDATE	√	-	-	-
SEARCH & MATCH	√	√	√	√
IDENTIFICATION	-	-	-	√

√ = APPLIES

Figure 5-2. Accuracy Requirements

	RESP. TIME									
SUBSYSTEM	MAXIMUM	AVERAGE	AVAILABILITY	CAPACITY	ACCURACY	OBSERVABILITY	OPERABILITY	MAINTAINABILITY	INTEGRITY	SECURITY
DATA COLLECTION	√	√	√			√	√	√	√	√
DATA ENTRY	↓	↓	↓		√	↓	↓	↓	↓	↓
SUBJECT SEARCH	↓	↓	↓	√	↓	↓	↓	↓	↓	↓
TECHNICAL SEARCH	↓	↓	↓	√	↓	↓	↓	↓	↓	↓
IDENTIFICATION/ VERIFICATION	↓	↓	↓	√	√	↓	↓	↓	↓	↓
RESPONSE GENERATION	↓	↓	↓			↓	↓	↓	√	↓
SYSTEM SUPERVISOR	√	√	√	√		√	√	√		√

√ = APPLIES

Figure 5-3. Applicable Performance Requirements

SECTION VI

INTERFACE REQUIREMENTS

The performance requirements listed in the measures of effectiveness that apply to interface requirements are the capacity for data, documents, or other pieces of information that pass from one subsystem to another or from the external world into the system. The performance requirements that also apply are operability, security, reliability (which can be included as part of availability), observability, and maintainability (see Figure 6-1).

Interfaces between subsystems and between the system and the external world are defined as those places in the systems where the two subsystems meet. They have a physical reality; however, it is assumed that no processing goes on within the interface and that no storage is available. Any buffering or storage required is performed by the interfacing subsystems themselves rather than the interface. Consequently, storage capacity requirements do not apply to interface requirements. Temporary capacity and average response time can be lumped together because there is no queue. The temporary capacity/response time requirements in Figure 6-1 have been derived from the design work load[4] required by the FBI for AIDS III.

Similarly, since there is no processing performed in the interface, accuracy does not apply.

Maximum response time also is not applicable to interfaces since without processing or storage there is no delay assumed in the interface.

To determine this applicability of performance, interfaces were typed as follows: fingerprint card and document interfaces, computer data interfaces, external interfaces, internal interfaces, and the special interfaces provided to the System Supervisor and Technical Support Subsystem. After examination it was discovered that the Technical Support Subsystem interfaces are not areas of system design and consequently though important are not applicable to this document. System Supervisor subsystem interfaces are all computer data interfaces and consequently can be put into that category. Similarly, inspection of the interface charts (Figures 4-1 through 4-9) shows that internal interfaces are all fingerprint card and document interfaces and consequently can be placed in those categories.

External interfaces will change if the present system, which employs mail both to and from the external world, is replaced by one that distributes processing or communications to the field employing

[4] "AIDS III Design Guidelines," attachment to letter from N. F. Stames, Assistant Director, Identification Division, Federal Bureau of Investigation, to R. E. Hilderbrand, Rockwell International, October 26, 1979.

	CAPACITY/ RESPONSE TIME[a]	OBSERVABILITY	SECURITY	RELIABILITY/ AVAILABILITY	OPERABILITY	MAINTAINABILITY
SYSTEM						
EXTERNAL						
DATA COLLECTION - USERS/CONTRIBUTORS	2993	√	√	√	√	√
DATA ENTRY - USERS/CONTRIBUTORS	2400					
RESPONSE GENERATION - USERS/CONTRIBUTORS						
INTERNAL						
DATA COLLECTION - CIVIL FILE	145					
DATA ENTRY - CIVIL FILE	128					
DATA ENTRY - MANUAL FILE	1952/609					
RESPONSE GENERATION - CIVIL FILE	238					
RESPONSE GENERATION - ARCHIVAL CRIMINAL FILE	837					
RESPONSE GENERATION - MANUAL SYSTEM	6[b]					
SUBSYSTEM TO SUBSYSTEM						
FINGERPRINT CARDS & DOCUMENTS						
DATA COLLECTION - DATA ENTRY	8755					
DATA ENTRY - TECHNICAL SEARCH	1187					
DATA ENTRY - IDENTIFICATION/VERIFICATION	939/294					
DATA ENTRY - RESPONSE GENERATION	143					
TECHNICAL SEARCH - RESPONSE GENERATION	282					
TECHNICAL SEARCH - IDENTIFICATION/VERIFICATION	1033/128					
IDENTIFICATION/VERIFICATION - RESPONSE GENERATION	468					
COMPUTER DATA						
SYSTEM SUPERVISOR - DATA ENTRY	3755					
SYSTEM SUPERVISOR - SUBJECT SEARCH	3110					
SYSTEM SUPERVISOR - TECHNICAL SEARCH	1187					
SYSTEM SUPERVISOR - IDENTIFICATION/VERIFICATION	1233	▼	▼	▼	▼	▼
SUPERVISOR - RESPONSE GENERATION	2530	√	√	√	√	√

√ = APPLIES

[a] AVERAGE TRANSACTIONS PER HOUR (FROM FIGURE 4-1, AIDS III OPERATING CONCEPT, IN REFERENCE 4)

[b] PLUS CARD INDEXES

Figure 6-1. System Interface Requirements

electronic transmission across the country. In this case a reexamination of the Data Collection, Data Entry, and Response Generation Subsystems will arise because of the time required to transmit data. However, they could be accommodated within the existing set of functions.

Consequently, the distinctions between interface types can be ignored since the basic six performance measurements listed above apply in every case and thus distinctions between interface types are not important. Also, it is clear that no more than these six performance requirements apply to interfaces given the definitions and assumptions listed above.

SECTION VII

GENERAL REQUIREMENTS

A. COMPUTER REQUIREMENTS

The principal purposes of this section are:

(1) To provide a system design approach to computer-based subsystems.

(2) To establish functional requirements for computer-based subsystem design.

(3) To establish general interface requirements for computers within the system.

1. Basic Requirements

The following are the basic requirements for computer-based subsystems:

(1) Integrated control inputs and displays to allow operation of multiple devices from a single station console.

(2) All hardware, software, and documentation to be standardized.

(3) Computer-to-computer communications to be standardized including areas of:

(a) Hardware: Message switch controller.

(b) Protocol: Communications procedures.

(4) Each processor to perform a single data system-related set of control, data processing, and analysis functions.

(5) Functions to be performed in a data-driven mode with no manual intervention, except for initialization, mode change, and reaction to alarms.

(6) Appropriate computers to be equipped with mass storage used for:

(a) Temporary data storage.

(b) Initialization values.

(c) Program retention.

(7) Individual computers to be capable of recovering from power interruption by means of:

(a) Own disk (where equipped).

(b) Subsystem processor's disk.

(c) Nonvolatile, outage-protected memory (e.g., read-only memory).

(8) Redundant computers able to be switched to functions for backup under System Supervisor control.

(9) Redundant processors to be used for critical data paths.

(10) Backup processors to be fully initialized and ready to begin processing.

(11) All processors to be capable of independent, stand-alone operation; no single failure to affect any other processor except for the interruption of data flow from the failed processor.

(12) Appropriate subsystem processor to be equipped with a printing device that can provide a permanent record of normal operations and diagnostics.

(13) Each subsystem processor to be capable of providing subsystem performance data, configuration data, and diagnostic messages to a display device at the central station console.

2. Standardization

a. Computer Classifications. For the purposes of standardization, computers may be divided into three classes. These classes are defined as:

(1) Microcomputers: Very small computers intended for control of a single assembly of a portion of a subsystem with limited data processing capability.

(2) Minicomputers: Small computers intended for subsystem control and capable of significant data processing.

(3) Large computers: Sizable computers intended for extensive data processing including multi-processing.

b. Standard Design. All processors within each of the three classes should be a standard design, with standard peripherals. This permits:

(1) Interchangeability between assemblies and peripherals.

(2) Commonality of software routines and subroutines.

(3) Maintainability.

(4) Minimum spares.

(5) Minimum training when new processors are introduced.

This requirement would be tempered to achieve the most reliable, cost effective system design.

All program initialization, operation, and documentation should be standardized to reduce operator training time and minimize operational errors. In particular, the operator-computer interface should be standardized. For example, operator type-ins, computer mnemonics, and the protocol between the operator and the computer should be standardized.

3. Modular Design

All implementations involving the use of computers should be of a modular design with as much standardization as possible. The concept of modularizing and standardizing equipment is useful because it provides the maximum flexibility in equipment replacement and the smallest inventory of spares.

4. Stand-Alone Capability

All processors should have the capability of stand-alone operation. Such operation should include boot-strap loading (initial loading of a processor with a blank memory), program loading, and entry of operational parameters. The boot-strap loading of all processors in their stand-alone mode should be accomplished by the use of firmware (read-only memories which are non-volatile), a keyboard device, and/or a mass storage device. Program loading and entry of operational parameters should be accomplished by a keyboard device and/or a mass storage device. Portable, roll-around terminals may be used for maintenance and checkout. However, all devices needed to operate a processor in its stand-alone mode must be permanently attached. In addition, a printing device may be required to permanently record normal operations and diagnostics.

When control is accomplished from the System Supervisor, the message provided will indicate the program for the subsystem processor to select from its own mass storage device rather than sending the entire program through the communications lines. The operational parameters would be sent along with the message selecting the particular program to be used. All programs would have default values, which include the parameters most likely to be used.

5. Subsystem Configuration and Mode Selection

The selection of the subsystem configuration and mode should be performed by the subsystem processor for that subsystem. (Configuration here means the interconnection of various assemblies in the data stream.)

The mode of operation is the particular operating method associated with a particular data mode.

6. Closed-Loop Control

Functions performed by servomechanisms requiring closed-loop control should be implemented so that control remains within the subsystem.

7. Safety Limits

All computer-controlled functions involving human or equipment safety should be provided with functionally redundant backups. The design should be such that a failure of the computer can in no way cause injury to personnel or damage to equipment.

8. Automatic Calibration

All computerized subsystems should have the capability to perform pre- and post-work shift calibration of all assemblies in the subsystem.

9. Fault Detection and Isolation

All computerized subsystems should include software with the capability to perform self-testing, and automatic fault detection and isolation to the replaceable module level. This capability should exist both during prepass calibration and during actual operations.

All subsystems should be capable of self-testing of all internal controls and responses.

10. Real-Time Diagnostics

The subsystem processor should continuously monitor all assemblies under its control, all its peripheral devices, and itself. An anomaly or failure should be logged and provided in an abbreviated form to the operators.

a. General Diagnostic Message Requirements. Diagnostic messages for assemblies under the control of the subsystem processor should at least identify the source of the anomaly or failure and, to the extent possible, describe the nature of the problem. Diagnostic messages for the computer peripheral devices and for the processor itself should include:

(1) Memory address of the instruction last accessed before the problem occurred.

(2) Contents of the program register at the time of anomaly.

(3) Subroutine being executed at time of anomaly.

(4) Process being executed when anomaly occurred.

In addition, if the nature of the problem warrants, the contents of all volatile registers in the computer should be listed. Where possible, a walk-back describing the subroutine calls which led to the occurrence of the problem should also be provided.

The diagnostic messages need not be in complete English text. The use of codes that can be identified and described more fully in an operating manual can be used to minimize the length of the actual diagnostic messages printed out.

b. Specific Diagnostic Message Requirements. In addition to the general information listed in paragraph 10.a., a specific diagnostic message should include, but not be limited to, the following specifics:

(1) Input/Output Device Error: The device and the nature of the problem should be included along with the process under execution when the error occurred. It should be stated whether the computer was reading or writing, and whether the error occurred in the peripheral device or internal to the processor. In addition, any attempt to read or write from devices not implemented with the particular processor should be identified.

(2) Illegal Operation: Any illegal operation should be identified.

(3) Guard Mode: When application software attempts to access memory locations outside of its designated memory allocation, a guard mode message should be generated.

(4) Arithmetic Error: Divide overflow, floating point characteristic overflow or underflow, and other arithmetic errors should produce diagnostic messages.

11. Error Control

Computer-to-computer communications (within one facility) should provide reliable data transfer with a probability of an undetected bit error occurring not to exceed one in 10^9. Detected errors should be logged automatically in a permanent form. The processor detecting the error may either request retransmission of the data block in error from the transmitting processor and/or generate an alarm that data have been received in error.

B. OPERATIONAL REQUIREMENTS

1. Rapid Calibration and Turnaround

Design should be such that pre-work shift calibrations may be accomplished for the entire operating system within TBS minutes and work shift calibrations with TBS minutes. Reconfiguration without pre- or post-calibration shall be accomplished in TBS minutes.

2. Reliability and Maintainability

Reliability should be a principal goal and can be achieved through the use of both intrinsically reliable equipment and redundancy. Redundant computers should be used in all cases where communications are critical.

C. STANDARDS

1. Hardware

Hardware standards should be in accordance with applicable Bureau and federal standards TBS.

2. Software

Software standards should be in accordance with applicab Bureau and federal software development standards TBS.

3. Testing

Each subsystem must be capable of being tested on a small scale before implementation on a large scale. Testing should be in accordance with applicable Bureau and federal standards TBS.

4. Transfer to Operations

Transfer to operations should be in accordance with Bureau standards TBS.

5. Documentation

Training, operations, and maintenance manual should be in accordance with applicable Bureau and federal standards TBS.

D. TECHNICAL SUPPORT

There is a requirement that the systems, both hardware and software, be supported by technical people who can perform maintenance on the current system and plan and implement new systems as needed.

E. FORECASTING AND RESPONDING TO ENVIRONMENT

It is important to monitor the changing climate for identification services and to consider the impact of these changes on equipment, personnel, and facilities.

1. Growth

From time to time special requests are initiated by the courts, the Congress, and other agencies such as the White House. These non-routine operations can vary from the clearance of special visitors to the White House to the requirement to expunge large numbers of records from the criminal file due to redefinition made by the courts of the appropriateness of the file. The ability to accurately estimate the impact of all special requests is important since it allows for the orderly management of resources and the estimation of budget impact of each special request.

2. New Requirements

The ability to accurately estimate the impact of all new requests is important since it too allows for the orderly management of resources and the estimation of budget impact of each request.

REFERENCES

1. FBI Identification Automation Study: AIDS III Evaluation Report, Vol. VII, Top Down Functional Analysis, JPL Pub. 80-79, Jet Propulsion Laboratory, Pasadena, California, August 1980.

2. Automation of FBI Identification Functions Feasibility Study: Revised Task Plan, 5030-456, Jet Propulsion Laboratory, Pasadena, Calif., September 1979 (internal document).

3. FBI Identification Automation Study: AIDS III Evaluation Report, Vol. V, Current System Evaluation, JPL Pub. 80-79, Jet Propulsion Laboratory, Pasadena, California, August 1980.

4. Hoban, T., and Burgard, J., Revised AIDS III Work Loads, AIDS Technical Memo 80-007J, Rockwell International, May 1, 1980.

APPENDIX

ACRONYMS

ACS	Automated Classification System
AFRS	Automated Fingerprint Reader System
AHU	Anti-Halation Underlayer
AIDS	Automated Identification Division System
ANS	Automated Name Search
ATS	Automated Technical Search
ATSPS	Automated Technical Search Pilot System
AUTOCOR	Automated Correspondence Station (part of AIDS)
AUTORESP	Automated Response Generation (part of AIDS)
A&R	Automation and Research Section of Identification Division
BER	Bit Error Rates
BLO	Blocking Out
CCA	Computerized Contributor Abbreviated Name
CCH	Computerized Criminal History (part of NCIC)
CCN	Computerized Criminal Name
CCNR	Computerized Criminal Name and Record (part of AIDS)
CCR	Computerized Criminal (Arrest) Record (part of AIDS)
CIR	Computerized Ident Response File (part of AIDS)
CLASS-A	Classification-A
CLASS-B	Classification-B
CLASS-C	Classification-C
CLCK	Classification Check
CNR	Computerized Non-Ident Response File
COA	Cutoff Age
CPU	Central Processing Unit

CRS	Computerized Record Sent File (part of AIDS)
CRT	Cathode Ray Tube
CSORT	Centerline Sort
DATE STP	Date Stamp, Count and Log
DBMS	Data Base Management System
DEDS	Data Entry and Display Subsystem (part of AIDS III)
DENT	Data Entry
DENT-A	Data Entry-Cards
DENT-B	Data Entry-Documents
DOA	Date of Arrest (on f/p card)
DOB	Date of Birth (on f/p card)
ECL	Emitter Coupled Logic
EMI	Electromagnetic Interference
ENC	Encode Input Data-Cards
ENCDOC	Encode Input Data-Documents
ENCK	Encode Check-Cards
ENDOCK	Encode Check-Documents
ERR	Update Error File
EYE	Color of Eyes (on f/p card)
FBI	Federal Bureau of Investigation
FEP	Front End Processor
FIFO	First-In-First-Out
FLAB	Film Lab Processing/Computer
FLOAD	Film Load
FPC	Fingerprint Classification
FPCS	Fingerprint Correspondence Section of the Identification Division
f/p	Fingerprint

GDBMS	General Purpose Data Base Management System
GEO	Geographic Location (on f/p card)
GPSS	General Purpose Simulation System
HAI	Color of Hair (on f/p card)
HGT	Height (on f/p card)
IBM	International Business Machines Corporation
ICI	Image Comparison Identification
ICRQ	Image Comparison Request
ICS	Image Comparison Subsystem (part of AIDS III, actually used for image retrieval for manual comparison)
ICV	Image Comparison Verification
ID, I.D.	Identification Division
IDENT	Identification
JPL	Jet Propulsion Laboratory
KIPS	Thousands of Instructions per Second (as executed by a computer)
LEAA	Law Enforcement Assistance Agency
MAIL	Open Mail and Sort
MFILM	Image Capture Microfilm
MIPS	Millions of Instructions per Second (as executed by a computer)
MMF	Minutiae Master File
MOE	Measures of Effectiveness
MTBF	Mean Time Between Failures
MTR	Master Transaction Record
MTTR	Mean Time to Repair
NAM	Name (on f/p card)
NASA	National Aeronautics and Space Administration
NCIC	National Crime Information Center

NCR	National Cash Register Company
OCA	Local Identification Number (on f/p card)
OCR	Optical Character Recognition
OMB	Office of Management and Budget
ORI	Originating Agency Identification Number (on f/p card)
PCN	Process Control Number
PICS	PCN and Image Capture Subsystem (part of AIDS III)
PMT	Photomultiplier Tubes
POB	Place of Birth (on f/p card)
QC	Quality Control
QUERY	On-Line Query
RAC	Race (on f/p card)
READ	Quality Control Check, Read, Annotate
RFI	Radio Frequency Interference
RH	Relative Humidity
RVF	Ridge Valley Filter
SACS	Semi-Automatic Classification System
SAR	Semi-Automatic Fingerprint Reader
SEAR	Search Review
SEX	Reported Sex of a Subject (on f/p card)
SID	State Identification Number
SKN	Skin Tone (on f/p card)
SOC	Social Security Number (on f/p card)
SPM	Search Processor Module
SS	System Supervisor Subsystem (part of AIDS III)
SSM	Subject Search Module
SSRG	Subject Search and Response Generation Subsystem (part of AIDS III)

TDFA	Top Down Functional Analysis
TFC	Technical File Conversion
TR	Transaction Record
TRC	Transaction Control File
TSS	Technical Search Subsystem (part of AIDS III)
TTL	Transistor - Transistor Logic
VDENT-A	Verify Data Entry-Cards
VDENT-B	Verify Data Entry-Documents
VLSI	Very Large Scale Integration
WAND	Wand Out of System